

Cloud computing: Anàlisi i disseny de l'estructura informàtica d'una empresa

Omar Kouyate Gabriel

Resum— La tecnologia cloud computing s'han convertit en una solució cada cop més habitual per a empreses que volen aprofitar els avantatges que aporta tenir el seu CPD localitzat al cloud, no obstant dur a terme aquesta solució requereix d'un anàlisi previ personalitzat per a cada empresa. Aquest article proposa l'estudi i la presa de decisions en el disseny de l'estructura informàtica d'una empresa que necessita realitzar un canvi en la seva infraestructura. En el cos de l'article es mostrarà un abstracte amb els punts claus que cal tenir en compte en el procés de migració dels serveis locals d'una empresa cap al cloud, una descripció sobre els conceptes bàsics que cal conèixer per realitzar un projecte d'aquestes característiques, s'explicarà com s'ha realitzat la implementació de la solució plantejada i finalment s'extrauran les conclusions obtingudes. La motivació de realitzar aquest treball, ha estat assolir una metodologia de treball i els conceptes globals de les Infraestructures com a servei, per aplicar-los en casos reals d'empreses que requereixin migrar part o la totalitat de la seva infraestructura al cloud.

Paraules clau— cloud computing, IaaS, cloud, AWS, CPD, VPC, migració, Infraestructura, núvol, Servidors.

Abstract—Cloud computing Technology have become a common solution for companies who want to exploit the advantages of locating their data center in the cloud. This solution requires to realize a customized analysis depending on the company. This article proposes the study and the decisions that have to be taken to design the network structure of a company that needs to improve their infrastructure. This article will show an abstract with the key points to consider when a local services migration has to be done, including a description of the basic concepts about cloud computing and the explanation of the proposed solution implementation, finally it will show the conclusions found. The motivation of this project has been to achieve a working methodology and the global concepts about an Infrastructure as a service, to apply them in real cases of companies that need to migrate all or part of its infrastructure to the cloud.

Index Terms—cloud computing, IaaS, cloud, AWS, CPD, outsourcing, infrastructure, Servers.



1 INTRODUCTION

En els últims anys, cada cop són més les empreses que decideixen abandonar el model tradicional d'infraestructura, i aposten per migrar part o la totalitat de la seva estructura de xarxa cap al núvol. En aquest procés de canvi, la majoria de les empreses necessiten contractar serveis de especialistes capaços de prendre decisions sobre quina és la millor manera de formar la nova infraestructura, quins elements de xarxa necessiten migrar al núvol, quins elements nous cal contractar, com configurar els servidors en el cloud, millorar la eficiència, reduir costos de manteniment etc.

Aquest projecte, neix per donar servei a les empreses que volen millorar la seva infraestructura de xarxa per aprofita-

tar les avantatges que proporciona una IaaS i no quedar obsoletes. Per a realitzar el treball s'ha realitzat un cas d'ús simulant la demanda de una empresa que vol portar el seu CPD al cloud, per tant s'ha hagut de crear una topologia de xarxa de l'empresa en qüestió especificant els servidors dels que disposa, els serveis que utilitzen i la seva disposició. Basant-se en els conceptes lligats a una infraestructura en cloud com escalabilitat, seguretat, rendiment, eficiència o disponibilitat, s'ha realitzat un anàlisi per a determinar la topologia final de l'empresa, decidint per a cada servei si convé portar-lo al cloud, mantenir-lo al CPD o substituir-lo per una millor solució.

Prèviament a la elaboració del cas d'ús s'ha realitzat una documentació sobre conceptes bàsics sobre cloud computing i la seva aplicació a les empreses, i s'ha realitzat una comparació entre diferents proveïdors de IaaS. Per a realitzar la comparació s'han escollit els tres proveïdors amb més cota de mercat actualment Amazon Web Services, Microsoft Azure i Google Compute Engine. Finalment s'ha realitzat un model d'implementació de la

-
- E-mail de contacte: omar.kgabriel@gmail.com
 - Menció realitzada: Enginyeria de computadors
 - Treball realitzat per: Omar Kouyate Gabriel
 - Curs 2015-2016

topologia final de l'empresa, contactant els servidors i elements de xarxa necessaris i comunicant la xarxa virtual creada al cloud amb la xarxa local de l'empresa. Per motius de temps i de recursos disponibles, s'ha decidit realitzar una implementació reduïda, implementant només els serveis necessaris per al funcionament del servidor App_Server, que executa l'aplicatiu ERP que utilitza l'empresa per gestionar productes, magatzem, vendes, contractes etc.

1.1 Objectius

L'objectiu del projecte és documentar l'anàlisi realitzat sobre la implementació de solucions cloud computing en les empreses, i la elaboració d'un cas d'ús per a una empresa en concret. Caldrà redactar els passos seguits per a les decisions preses respecte l'externalització del cpd i la modificació de la topologia de xarxa.

Finalment es realitzarà la implementació del cas d'ús proposat i es realitzaran proves de rendiment, comparant la comunicació entre servidor cloud i servidor físic per a obtenir informació que es valorarà a les conclusions del projecte.

TAULA I. LLISTAT D'OBJECTIUS DEL PROJECTE

Objectius	Prioritats
Documentació sobre l'aplicació de cloud computing a l'empresa	Prioritari
Comparació entre proveïdors de cloud computing	Secundari
Definició de l'empresa client	Crític
Requisits de l'empresa client	Prioritari
Documentació sobre el proveïdor de IaaS	Prioritari
Decisió de la nova infraestructura de xarxa	Prioritari
Implementació de la infraestructura de xarxa	Prioritari
Realitzar el projecte en el termini especificat	Crític

Fig1. Llistat d'objectius de cloud computing: anàlisi i disseny de l'estructura informàtica d'una empresa

1.2 Contingut

Aquest article conté els següents apartats.

- Introducció
- Estat de l'art
- Metodologia
- Planificació
- Cloud computing
- Empresa client
- Virtual private cloud
- Implementació
- Conclusions
- Bibliografia

1.3 Estat de l'art

Actualment són moltes les empreses que decideixen canviar la seva infraestructura de xarxa física i aprofitar la tecnologia cloud computing per a obtenir millor eficiència econòmica, millor disponibilitat, seguretat o rendiment part o la totalitat del seu CPD al núvol. Per a poder realitzar la migració al cloud de manera òptima cal dur a terme un anàlisi previ sobre la infraestructura de la empresa i decidir quina solució aplicar depenent dels requisits d'aquesta i de les limitacions de la tecnologia.

Actualment existeixen multitud de proveïdors d'infraestructures de xarxa com a servei, aquest proveïdors ofereixen la possibilitat de instal·lar servidors virtuals o dedicats que es configuraran i gestionaran a través de internet,

2 CLOUD COMPUTING

2.1 Definició i conceptes bàsics.

Cloud computing és una tecnologia que ofereix serveis de còmput a través de internet. La base principal d'aquesta tecnologia és que els processos de còmput es realitzen en servidors externs, d'aquesta manera els usuaris no requereixen de un hardware específic per executar aplicacions, allotjar serveis, bases de dades etc.

Quan parlem de cloud computing, podem diferenciar entre tres categories en funció del nivell d'abstracció ofert al usuari final.

Software as a Service SaaS:

Parlem de SaaS quan un proveïdor de software ofereix una aplicació als usuaris a través de internet, aquest proveïdor s'ocupa del manteniment i el correcte funcionament de l'aplicació, i els usuaris s'hi connecten simplement per utilitzar les funcions que ofereix.

Exemples de SaaS: Gmail, Basecamp, Moodle, Facebook, Twitter.

Platform as a Service PaaS:

Platform as a Service és un model de cloud computing on els proveïdors ofereixen un espai als desenvolupadors per a crear i gestionar les seves aplicacions.

Exemples de PaaS: Google Apps Engine, Apprenda, Velneo.

Infrastructure as a Service IaaS:

IaaS ofereix una infraestructura on els usuaris poden allotjar servidors, bases de dades, sistemes d'emmagatzematge etc. Els proveïdors de IaaS ofereixen un sistema de contractació escalable on només pagues pels recursos utilitzats (ús de CPU, capacitat d'emmagatzematge, velocitat de transferència etc.)

2.2 Proveïdors de IaaS

Aquest projecte es basa en l'aplicació de un IaaS per a configurar la infraestructura d'una empresa, per tant s'ha basat l'estudi en els diferents proveïdors de IaaS existents per a realitzar la implementació. Per a realitzar l'estudi s'han escollit els 3 proveïdors amb més cota de mercat actualment Amazon Web Services, Microsoft Azure i Google Compute Engine, cal dir que existeixen un gran nombre de proveïdors de IaaS, però s'han escollit els tres anteriorment esmentats per la confiança i seguretat que aporten al client al ser grans empreses conegudes per tothom.

El funcionament dels serveis oferts per aquest proveïdors és molt similar, ja que els tres ofereixen la possibilitat de contractar servidors virtuals amb un hardware preconfigurat els quals se'n paga la utilització en hores. La disponibilitat que garantitzen aquests proveïdors és pràcticament idèntica, d'un 99.5%, tot i que en els darrers dos anys Amazon Web Service ha estat el proveïdor que ha ofert una millor disponibilitat amb un temps de caiguda de 2h 30 minuts, respecte les 10h i 50 minuts de Microsoft Azure i les 11h i 35 minuts de Google Compute Engine.

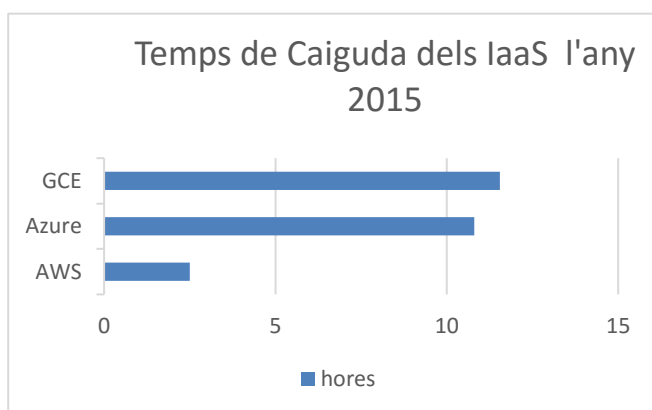


Fig2. Comparació de temps de no disponibilitat dels IaaS Durant l'any 2015

Si que hi ha un canvi significatiu entre els proveïdors en qüestió de preu dels productes, a la figura 3, es mostra un gràfic representatiu dels preus de contractació d'una instància Windows durant un mes en els diferents proveïdors analitzats.

si es desitja contractar instàncies d'alt rendiment amb molta capacitat de còmput i memòria ja sigui per executar operacions complexes, configurar servidors de grans prestacions etc. Google Cloud Platform és la opció més econòmica, en canvi per a instàncies de propòsit general o servidors mitjans, Amazon Web Service esdevé la millor opció econòmicament parlant.

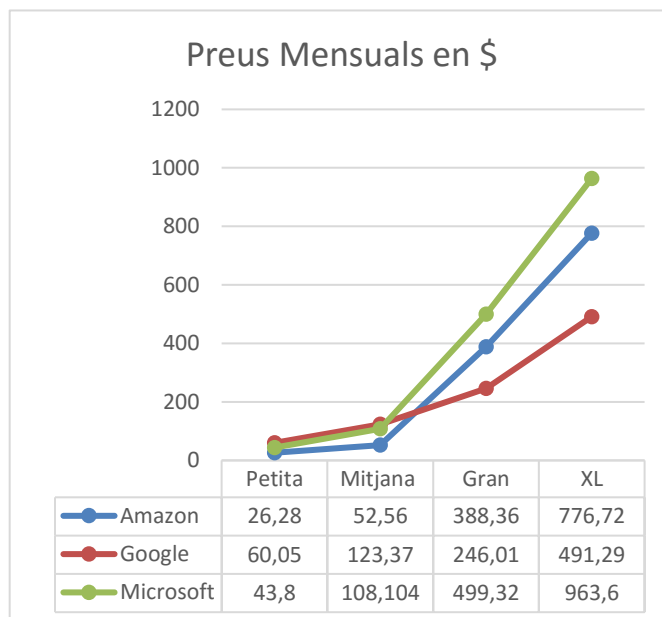


Fig3. Comparació de preu mensual entre Instàncies de diferents proveïdors

2.3 Decidir Proveïdor IaaS

Amazon Web Service és el proveïdor de IaaS amb més cota de mercat i el que porta més anys oferint aquest servei, com conseqüència disposa de més opcions de configuració, més serveis addicionals relacionats amb l'IaaS així com més acords amb tercers que proporcionen instàncies amb software configurat com per exemple Bussines SAP, OpenBravo, SoftNaS. Degut a aquestes avantatges i al preu reduït de les seves instàncies, s'ha decidit utilitzar Amazon Web Service com a model de proveïdor de IaaS per a realitzar la implementació d'aquest treball i així poder aprofundir en el funcionament del proveïdor més utilitzat en el mercat laboral.

3 METODOLOGIA

La metodologia seguida per a dissenyar la solució en cloud computing per a el cas d'ús plantejat, ha consistit en la definició de 6 fases, proposta d'un cas d'ús, Anàlisi dels requisits, disseny de la solució, implementació i proves. Un cop definides les fases de l'projecte s'ha seguit un desenvolupament en cascada per anar complint cada fase en el temps especificat. Aquesta metodologia es basa en tancar una fase abans de començar la següent, degut a les dependències entre fases, cal assegurar-se de que quan es dona per finalitzada una fase, no serà necessari modificar-la posteriorment.

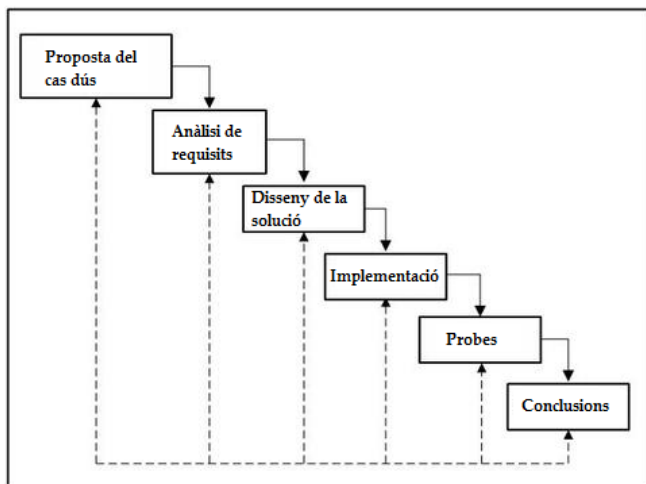


Fig4. Fases del desenvolupament del treball en cascada

4 PLANIFICACIÓ

Per a planificar el temps de desenvolupament de les fases del treball, s'ha realitzat una estimació de les hores necessàries per a finalitzar cada fase tenint en compte la data límit de finalització del projecte. S'ha utilitzat l'eina Microsoft Project per elaborar un diagrama de Gantt que s'ha seguit durant el termini de elaboració del treball.

5 DEFINICIÓ EMPRESA

Per a la elaboració del cas d'ús per a el projecte, s'ha simulat la petició d'una empresa que necessita modificar la seva infraestructura de xarxa, per a estalviar costos en manteniment i millorar la eficiència del seu cpd.

5.1 Resum de la situació de l'empresa client

Sportife és una empresa que es dedica a la venda de roba esportiva online, aquesta ha viscut un creixement significatiu en els últims 5 anys, ja que ha passat de ser un projecte de 5 socis a esdevenir una empresa que actualment compte amb 75 treballadors, arran d'això l'empresa Sportife es planteja una solució en cloud per a estalviar costos en infraestructura informàtica i tenir un sistema de dades més fiable, escalable i modern.

Actualment, L'empresa Sportife compta amb un conjunt de servidors que s'han anat comprant durant el creixement de l'empresa, aquests servidors, han estat configurats per una empresa informàtica externa, que els hi dona suport quan alguns d'aquests fallen o es necessiten ampliar els recursos.

L'empresa Sportife necessita una infraestructura de xarxa, que asseguri la alta disponibilitat del servidor web ja que és un servei crític per la seva economia i la opinió dels clients sobre la seva pàgina web, a més a més requereixen una solució que permeti escalar els servidors sempre que sigui necessari sense que això impliqui grans despeses en concepte de material, temps i disponibilitat. Adicionalment requereixen garanties en qüestió de seguretat dels servidors, especialment en la seguretat de la base de dades, que conté informació sensible sobre treballadors i clients.

reixen una solució que permeti escalar els servidors sempre que sigui necessari sense que això impliqui grans despeses en concepte de material, temps i disponibilitat. Adicionalment requereixen garanties en qüestió de seguretat dels servidors, especialment en la seguretat de la base de dades, que conté informació sensible sobre treballadors i clients.

5.2 Requisits

Requisits funcionals

- R1. L'empresa busca una solució per millorar la disponibilitat dels seus servidors, ja que amb la configuració actual no son capaços de assegurar una alta disponibilitat i consideren la seva infraestructura vulnerable a fallades. Caldrà assegurar la màxima disponibilitat dels servidors, especialment del servidor web, que en cap cas pot ser menor del 90%
- R2. Seguretat: Les polítiques de seguretat del servidor de base de dades han de complir l'establert per la llei de protecció de dades Espanyola.
- R3. Conservar Topologia: Cal mantenir les direccions IP dels elements de la xarxa local i realitzar les mínimes modificacions en la LAN de l'empresa, per tal de que el canvi resulti poc traumàtic pel servei tècnic d'aquesta.
- R4. Conservar Serveis: L'empresa sol·licita mantenir els mateixos serveis en els servidors cloud, instal·lar la mateixa versió de ERP i Apache per a facilitar la gestió d'aquests.

Requisits no funcionals:

- R5. Aïllament d'instàncies sensibles: Separar lògicament les instàncies amb informació sensible de les instàncies amb accés no restringit.
- R6. Comunicació xifrada: La comunicació entre instàncies cloud i la xarxa local es realitzarà a través d'un túnel VPN a través d'internet.
- R7. Amortitzar Hardware disponible: A l'hora de realitzar el disseny de la nova infraestructura cal tindre en compte opcions d'aprofitament del hardware de l'empresa.
- R8. Aprofitament de recursos: El hardware contractat al proveïdor de IaaS ha de ser adequat als serveis destinats.

5.3 Topologia

A continuació es mostra un diagrama de xarxa on es pot veure la topologia actual de l'empresa Sportife, en aquesta topologia cal destacar que els servidors web estan aïllats en una DMZ de la resta de servidors, això es degut a que aquests servidors són accessibles des de internet i per seguretat s'ha volgut separar-los dels altres servidors que només han de ser accessibles per als treballadors de l'empresa.

Els treballadors Utilitzen diferents subxarxes per a cada departament al que pertanyen , aquestes subxarxes van des de el bloc 192.168.30/24 al bloc 192.168.40/24.

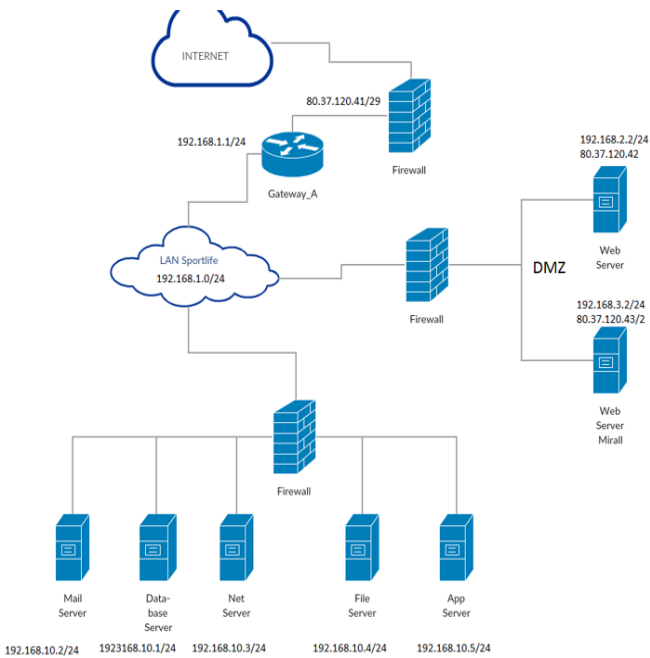


Fig5. Diagrama de xarxa de la topologia de l'empresa Sportife

Servidor	Descripció
Web Server	Aquest servidor allotja la pàgina web on accedeixen els clients per fer les compres. Apache Server.
Web Server Mirall	Un segon servidor web on es balanceja el tràfic d'usuaris en cas de que el servidor principal no tingui la capacitat de resoldre les sol·licituds o quedi fora de servei.
Mail Server	Apache Server. Servidor de correu de l'empresa, cada usuari té un espai reservat de 5 GB de capacitat.
Net Server	Exchange 2010, IIS7 Aquest servidor proporciona diferents serveis de xarxa i comunicació.
DATABASE Server	DHCP, DNS, Telnet, Active Directory. Emmagatzema la base de dades de l'empresa, conté informació sensible tant d'usuaris com dels empleats. Aquest servidor ha de ser accessible pel Web Server i per l'App Server.
File Server	MySQL. Cada empleat té reservats 20 GB de espai per a dades en aquest servidor. Quan un empleat inicia sessió al seu pc, automàticament es mapeja el seu directori remot propi i un directori departamental de mida variable segons el departament.
App Server	Share Message Block (SMB), Network File System (NFS) En aquest servidor s'executa una aplicació ERP que permet als treballadors gestionar el magatzem, vendes, contractes, proveïments etc. de l'empresa. També s'hi ha instal·lat un servei d'impressió i un servei de monitorització que recull mètriques sobre els recursos utilitzats, accessos i tràfic generat en els servidors WEB, Mail Server i DATABASE Server OpenERP, Cricket, Cups.

Fig6. Resum dels Servidors de l'empresa client.

En la següent taula es mostra un llistat dels servidors existents a la LAN de Sportife i una breu descripció sobre els serveis que ofereixen.

5.4 Solució plantejada

S'ha optat per a dissenyar una infraestructura mixta allotjant la majoria de serveis al cloud, però mantenint físicament els serveis que es poden ressentir al ser externalitzats.

Serveis migrats al cloud.

- Web server: s'aprofita la disponibilitat del 99.5% que assegura AWS per a mantenir el servei actiu i dependre de la dependència del servidor mirall. En cas de un gran demanda de accessos, s'aprofita la opció de autoescalada per a llençar un segon servidor que es pagarà les hores que estigui actiu.
- Active directory: AWS proporciona un servei d'administració de directoris que utilitza Samba 4 i proporciona un subconjunt de les capacitats que ofereix l'Active Directory de Microsoft com l'inici de sessió únic, gestió d'equips mitjançant dominis o gestió de grups basat en permisos.
- Dhcp i Dns: Aws dona la possibilitat de configurar les opcions dhcp i dns de forma gratuïta per a la xarxa virtual .
- Database: La data base de l'empresa augmenta en capacitat i complexitat constantment, utilitzant el servei RDS de amazon, es disposa d'una alta escalabilitat ja que es poden modificar els recursos del servidor en qüestió de minuts.
- ERP: S'instal·larà el sistema d'informació que utilitza l'empresa en una instància en cloud, d'aquesta manera s'incrementa la eficiència de la comunicació entre ERP al realitzar-se en un canal dedicat i no a través de internet.

Serveis mantinguts al cpd.

- Mail server: Degut a que el servidor no és susceptible de ser escalat en els pròxims anys, i no ser crítica la disponibilitat d'aquest, s'ha decidit mantenir el servidor de correu de l'empresa en la xarxa local i no portar-lo al cloud.
- DHCP: El servei DHCP que ofereix Amazon no permet servir la configuració de xarxa als elements fora de la xarxa virtual, per tant es mantindrà aquest servei en la xarxa local de l'empresa.

File Server.

- En el cas del sistema de fitxers de l'empresa, s'ha decidit una solució mixta. Es mantindrà el servidor File server a la xarxa local, i a l'hora s'instal·larà un altre a la xarxa virtual. Aprofitant la replicació DFS

de Microsoft es sincronitzaran els servidors assegurant la consistència de les dades.

Amb aquesta solució s'augmenta la disponibilitat del servidor de fitxers, s'incrementa l'eficiència en la recuperació de dades en cas de fallada, es supprimeixen les tasques de backup que es realitzaven a l'empresa i es dona la possibilitat a l'empresa d'amortitzar el hardware comprat.

6. VIRTUAL PRIVATE CLOUD

Una Virtual Private Cloud és una xarxa virtual que podem definir en AWS, aquesta xarxa és semblant a una xarxa típica de qualsevol empresa, i proporciona una infraestructura a les instàncies EC2 per a que es puguin comunicar a través de internet mitjançant un gateway de sortida. Podem dir que una VPC és la capa de xarxa de Amazon EC2.

Quan es decideix crear una nova VPC, Amazon EC2 ens proporciona una xarxa /16 per defecte 10.0.0.0/16 però es pot escollir el bloc CIDR que es vulgui, és en aquesta xarxa on es podrà començar a crear les subxarxes, taules de rutes, connexions vpn, nat gateways, definició de ips etc..

Quan es crea una VPC, aquesta per defecte no té sortida a internet, si volem habilitar la sortida a internet a els elements de la xarxa, s'haurà d'afegir un internet gateway a la VPC.

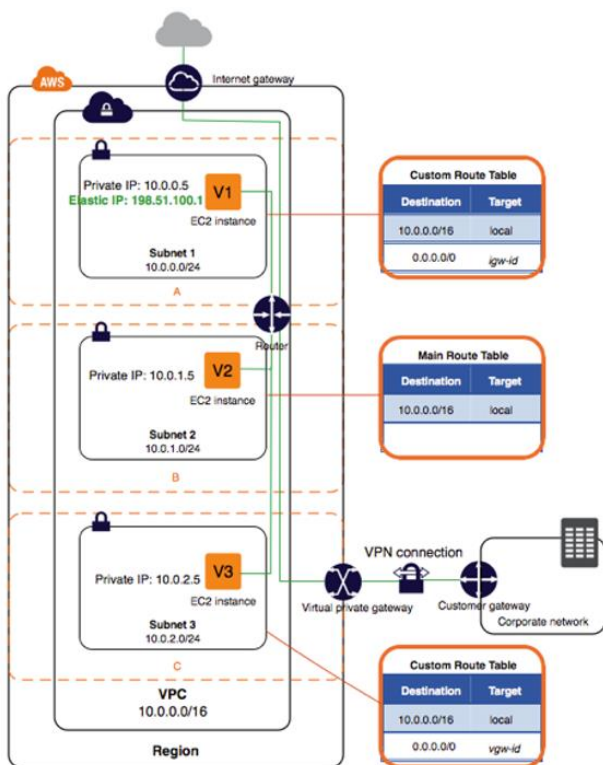


Fig7. Exemple de VPC connectada amb connectada via hardware VPN amb una xarxa local

6.1 Components d'una VPC

Regió:

La regió de la VPC és el lloc físic on està situat el datacenter de Amazon, actualment hi han 10 regions disponibles, 3 a estats units, 2 a Europa, 4 a àsia i 1 a sud Amèrica. Cada regió està físicament aïllada de les altres i només es poden comunicar via internet, quan es crea una VPC cal escollir en quina regió es vol crear.

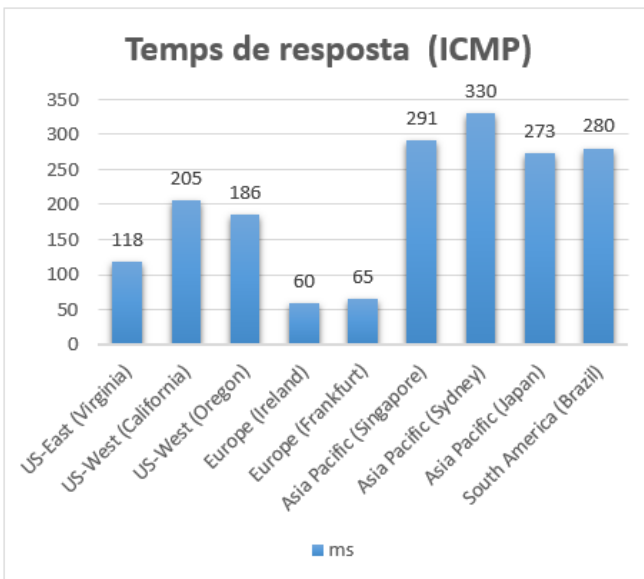


Fig8, Temps de resposta a instàncies en diferents regions des de Barcelona (Catalunya)

Depenent de la localització del datacenter i la localització del usuari s'obtidran diferents temps de resposta cap a les VPC de amazon, per tant a l'hora d'escollir una regió per allotjar les instàncies creades, caldrà decidir quina opció és la més eficient en temps de resposta / preu, ja que el pricing per a cada regió també es diferent.

Availability Zones:

Una Availability Zone, és una zona aïllada dintre d'una regió. Cada regió està formada per diferents AZ i cada AZ pertany a una sola regió, les AZ de una mateixa regió estan lògicament aïllades però connectades amb links de baixa latència.

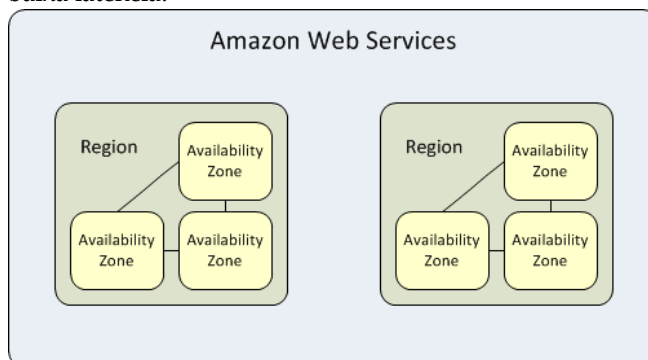


Fig9. Diagrama representatiu de la distribució de les AZ dins de les regions

Instàncies:

Una instància és un conjunt de recursos hardware, que lògicament funcionen com un únic terminal, AWS utilitza la virtualització en els CPDS per oferir diferents tipus d'instàncies segons els recursos dels que disposen, aquests tipus d'instàncies es classifiquen per famílies (optimització memòria, ús general, optimització de emmagatzematge, optimització GPU..)

Quan es crea una instància, s'escull una imatge (AMI) que formarà la base software de la instància, Amazon ofereix AMIS amb diferents sistemes operatius, però també es pot escollir una AMI pre-configurada amb software de tercers, com per exemple SAP, Drupal, OpenBravo etc.

Un cop creada la instància, s'hi pot configurar el software que esdesitgi. les instàncies poden ser duplicades per a que s'executin conjuntament, aquesta opció s'acostuma a aplicar creant grups d'autoescalament quan els recursos de la instància no són suficients com per assolir la demanda.

Route Tables:

En les taules rutes de la VPC s'especifiquen a on han d'anar dirigits els paquets d'una subxarxa depenent de la destinació final. Les taules de rutes s'apliquen a les subxarxes i cada subxarxa només pot estar associada a una taula.

Security Groups:

Un grup de seguretat, funciona com un Firewall virtual per a les instàncies de la VPC creada, quan es crea una VPC es crea també un grup de seguretat predeterminat, on es poden modificar les regles d'entrada i sortida que es volen utilitzar. Es poden crear diferents grups de seguretat per atorgar regles diferents segons les instàncies.

6.2 Comunicació entre VPC i LAN

En molts casos, es necessita connectar la VPC amb una o mes xarxes local del consumidor de IaaS, Amazon AWS proposa tres tipus de connexions VPN per a poder connectar aquestes xarxes.

-Hardware VPN: S'afegeix un Virtual Private Gateway en la VPC i es configura una connexió VPN entre aquest element i el Customer Gateway (endpoint de la LAN del client)

- AWS Direct: S'estableix una connexió de xarxa dedicada entre la LAN del client i la VPC d'Amazon, guanyant en seguretat i predicibilitat del canal de comunicació

- Software VPN: Connexió VPN entre un endpoint i una instància configurada com a servidor VPN, no es veu afectada per les limitacions hardware de les anteriors opcions, però la disponibilitat i la eficiència del canal recau en la configuració software realitzada.

7.IMPLEMENTACIÓ

La topologia final de la infraestructura de xarxa de l'empresa Sportife, estarà formada per una VPC on si crearan tres subxarxes en tres Availability Zones diferents, això proporcionarà seguretat en els servidors de SQL, FileServer y App server al estar lògicament aïllats del servidor públic Web Server, en aquesta VPC s'hi inclourà un Internet Gateway que comunicarà el WEB Server amb internet, i es contractarà un VPN gateway per establir una connexió dels demés servidors amb la xarxa de l'empresa.

La regió que s'ha escollit per a muntar la VPC ha estat EU(Irlanda) ja que l'empresa Sportife està situada a Catalunya i les seves vendes es concentren al continent europeu, d'aquesta manera s'aprofita la proximitat del servidor amb els usuaris, per obtenir un menor temps de resposta en les peticions.

7.1 Crear VPC

El primer pas per a muntar la infraestructura, es crear la xarxa virtual on s'instal·laran tots els elements del cloud. Per crear una VPC en AWS, únicament cal accedir a la consola de Amazon, anar al VPC dashboard i clicar Create VPC.

Després ens apareixerà un quadre on hem de donar el nom a la VPC i un CIDR block, i si es vol contractar un hardware dedicat per a la VPC.

7.2 CREAR SUBXARXES

El següent pas per a definir la infraestructura de xarxa plantejada, és crear les 3 subxarxes que formaran la VPC.

A la subxarxa A 10.0.1.0/24 estarà instal·lat el Web server de l'empresa, aquest web server tindrà una direcció IP privada, i se li afegirà una elastic IP (IP pública) per a poder ser accessible de internet.

S'ha decidit aïllar-la Subxarxa A en una Availability Zone diferent de les altres per qüestions de seguretat ja que el servidor web, rep milers de peticions diàries procedents de internet, algunes d'aquestes poden ser malicioses, buscant penetrar/infectar el servidor o altres elements de la xarxa. Aïllant el servidor WEB d'aquesta manera, protegim els altres elements de la infraestructura de l'empresa com el servidor de base de dades, file server o APP server.

En la subxarxa B 10.0.2.0/24 s'hi ha instal·lat el servidor de Base de Dades de l'empresa, separant aquest servidor del File Server i del APP server es busca protegir la informació crítica de la que disposa, d'aquesta manera s'evita que els treballadors, els quals tots ells poden accedir al servidor de fitxers, es mantinguin aïllats del servidor de base de dades.

En la tercera subxarxa de la VPC 10.0.3.0/24, s'hi configuraran dos servidors, el File Server i l'App Server, aquesta subxarxa serà accessible des de la LAN de l'empresa i no tindrà sortida a internet.

el procés per a crear una subxarxa és similar al procés de crear la VPC, només cal accedir al VPC dashboard → subnets → Create Subnet.

7.3 Afegir Internet Gateway

Per defecte, la VPC creada no té una porta d'enllaç que permeti la sortida a internet, en aquest cas necessitem una sortida a internet per a que el servidor WEB funcioni correctament, per això cal crear un Internet Gateway.

7.4 Afegir Virtual Private Gateway

Per interconnectar les xarxa local de l'empresa amb la xarxa virtual del cloud, s'ha decidit fer-ho mitjançant una connexió Hardware VPN, per això caldrà afegir un virtual private gateway (VPG) en la xarxa VPC i un gateway compatible amb el VPG per instal·lar-lo a la xarxa local. A la documentació de Amazon AWS es pot trobar un llistat de gateways compatibles per a establir una connexió hardware vpn amb la xarxa virtual creada.

7.5 Configurar la connexió VPN

La connexió VPN es una comunicació xifrada entre dues xarxes a través de internet, de manera que les xarxes simulin una topologia LAN. Els elements encarregats de comunicar aquestes xarxes són un Virtual Private Gateway a la part cloud de la infraestructura, i un Customer Gateway hardware a la part física. Aquests dos elements utilitzen els protocols IKE i Ipsec per a formar dos túnels de comunicació xifrada

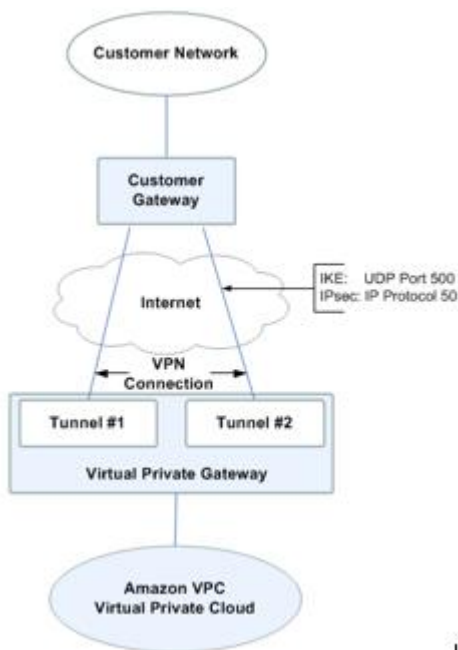


Fig10. Model de connexió VPN entre una VPC i una LAN

Per a configurar la connexió VPN entre la VPC i la xarxa local de l'empresa, s'ha de definir el customer gateway en la VPC especificant la ip d'aquest i el tipus d'enrutació que s'utilitzarà (Estàtica o dinàmica). Seguidament des de el dashboard de la VPC es crea la connexió VPN Especificant les dues xarxes a connectar. Per últim cal modificar les taules de rutes i els Security groups per a permetre la

comunicació entre les dues xarxes. Un cop fet això, la connexió VPN queda configurada a la part de la VPC.

Per a que quedi completament habilitada cal accedir al Costumer Gateway de la part de la LAN i crear els túnels vpn, especificant les direccions de cada túnel, la direcció del endpoint a la vpc, les restriccions del tràfic que viatjarà per la vpn i les subxarxes que es comunicaran.

Com que el costumer Gateway està situat darrere de un Firewall, cal definir les regles per a que es permeti el tràfic a través del Firewall entre els dos endpoints de la VPN.

7.6 Contractar les instàncies

Les instàncies són nodes virtuals amb un hardware específic dedicat i que executen el sistema operatiu seleccionat, per a muntar els servidors Web server, File Server, App Server i Database de la VPC s'han contractat 4 instàncies diferents. El cas d'ús implementat s'ha basat en la instal·lació del servidor App server que proporciona la aplicació ERP a la empresa.

Per a instal·lar el APP server en la VPC s'ha optat per contractar una instància denominada M3.large amb sistema operatiu Ubuntu Server 14.04 LTS, aquesta instància proporciona un equilibri entre capacitat de còmput i memòria que permetrà executar l'aplicació ERP de forma òptima.

7.7 Security Groups

S'han configurat tres security groups, que filtraran el tràfic que envien i reben les instàncies de cada subxarxa.

SG_A: es permet el tràfic http i https entre una instància i qualsevol altre destinació, permet la comunicació ssh entre una instància i la xarxa local de l'empresa. Aquest security group s'aplicarà al Servidor Web.

SG_B: Permet el tràfic TCP, UDP i ICMP entre una instància i els nodes de la VPC, permet el tràfic SSH entre una instància i la xarxa local de l'empresa. Aquest security group estarà associat al Database Server.

SG_C: Permet el tràfic TCP, UDP i ICMP entre una instància i el SG_B i la xarxa local de l'empresa. Aquest Security group estarà associat al APP Server i al File Server.

7.8 Instal·lació Odoo

Un cop creada la instància App Server, s'ha accedit a la màquina mitjançant una connexió ssh i s'ha instal·lat el servidor Odoo, el sistema ERP que utilitza l'empresa per a gestionar la seva informació. Un cop instal·lada la aplicació OpenERP, s'ha accedit al servidor via http pel port 8069, i s'ha comprovat que la web és accessible des de una instància VPC i desde una xarxa local a través d'internet.

7.9 Test de connexió.

Les instàncies de una VPC estan connectades entre si amb connexions de baixa latència que poden arribar a donar una taxa de 8.86 Gbps, L'ample de banda obtingut en una comunicació entre dues instàncies, dependrà de la regió on estiguin situades les instàncies i del tipus d'instàncies contractades. Les instàncies EC2 tenen 4 ni-

vells diferents de rendiment na la xarxa, nivell baix, moderat, alt i 10Gb.

Rendiment de comunicació	Ample de Banda
Baix	Fins a 100 Mbps
Moderat	De 100 a 300 Mbps
Alt	De 100 a 1.86 Gbps
10 GB	Fins a 8.86 Gbps

Fig11. Classificació del rendiment de xarxa de les instàncies

L'instància contractada per a allotjar l'aplicació ERP està dintre de la família d'alt rendiment de xarxa, per a comprovar que l'ample de banda és l'especificat per a aquesta família, s'ha realitzat un test de connexió entre la instància App_Server i una altre instància de la mateixa família utilitzant l'eina iperf, que calcula l'ample de banda mitjançant l'enviament de segments tcp entre un servidor i un client. L'ample de banda obtingut en el benchmark ha estat de 744Mbps i per tant es troba dins del límit especificat per a les instàncies d'alt rendiment de xarxa.

L'ample de banda en la comunicació entre la VPC i la LAN de l'empresa dependrà del proveïdor de IS que els hi proporcioni el servei.

8 CONCLUSIONS

Una Infraestructura as a Service, pot donar solució a les empreses que busquen millorar la escalabilitat, la disponibilitat i reduir les tasques de manteniment dels seus servidors.

Les empreses petites i mitjanes, normalment no disposen dels recursos necessaris per assegurar una alta disponibilitat dels serveis oferts i les polítiques de seguretat solen ser precàries en qüestions de prevenir amenaces externes que busquen corrompre els servidors o interceptar comunicacions. Per a aquestes empreses la migració dels serveis al cloud suposa un gran increment de la disponibilitat dels servidors. En qüestió de seguretat, es perd control sobre les dades ja que no estan allotjades físicament en la xarxa de l'empresa, però si s'escull un proveïdor de IaaS que ofereixi garanties en les seves polítiques de seguretat i es configuren correctament les regles de comunicació entre la xarxa virtual i l'exterior, s'obtindrà un entorn fiable i que compleixi els estàndards de seguretat definits per a emmagatzemar dades sensibles. Al contrari que en una xarxa física local, el rendiment dels servidors no està limitat al hardware disponible, en un entorn de IaaS es poden incrementar els recursos en qüestió de segons i així mantenir el rendiment i evitar la saturació dels servidors en moments de alta demanda.

Els proveïdors de infraestructures estudiats, AWS, Windows Azure i Google Compute Engine, ofereixen un entorn intuïtiu on crear els elements de xarxa necessaris per a obtenir la infraestructura desitjada, si es tenen clars els conceptes de com funcionen les instàncies, gateways i seguretat en el cloud, es pot crear una infraestructura de xarxa en un temps molt reduït. La comunicació entre la xarxa virtual i la xarxa local de l'empresa és l'aspecte crític a l'hora de configurar la infraestructura, cal assegu-

rar una comunicació segura i a l'hora eficient entre els elements de les dues xarxes.

La instal·lació de l'aplicació ERP en la instància App server configurada s'ha realitzat a través de una comunicació SSH i seguint els mateixos passos que es seguirien en un servidor local, l'accés a l'aplicació ERP un cop instal·lada s'ha realitzat a través d'internet, i per tant s'ha vist incrementat el temps de resposta de les peticions, aquesta increment del temps de resposta es perceptible en l'establiment de la comunicació amb el servidor, però es despreciable en la navegació per a l'entorn web.

Un servei de disseny de infraestructures cloud, tindria com a target empreses que necessitin assegurar la disponibilitat dels seus servidors, per exemple empreses dedicades a la venda de productes online o empreses amb un flux de tràfic irregular que necessiten una gran capacitat de recursos en moments determinats, per exemple en un servidor que ofereix el consum de vídeos online, en aquest cas es millora és la eficiència dels servidors en qüestió de rendiment/preu ja que només es pagaria el preu del hardware d'alt rendiment en els moments necessaris a costa d'un control la facturació dels recursos.

9. BIBLIOGRAFIA

- [1] Diversity Limited, "Understanding the cloud computing Stack."
http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf
[Data de consulta: Març 2016]
- [2] Amazon Web Service, "Elastic Cloud computing documentati-on".<https://aws.amazon.com/es/documentation/ec2/>
[Data de consulta: Abril 2016]
- [3] Microsoft Azure, "Microsoft Azure Documentation".
[Data de consulta: Abril 2016]
- [4] Vincent DAnen, "Lock IT Down: Implementing a DMZ"
<http://www.techrepublic.com/article/lock-it-down-implementing-a-dmz/>
[Data de consulta: Abril 2016]
- [5] everac99; 2008, "Alta Disponibilidad: Qué es y Cómo se logra"
<https://everac99.wordpress.com/2008/08/19/alta-disponibilidad-que-es-y-como-se-logra/>
[Data de consulta: Abril 2016]
- [6] Gladstone Health & Leisure Technical Services; Database ServerSpecs:
<http://www.gladstonemrm.com/Portals/2/Documents/Technical/Server%20Recommended%20Specifications.pdf>
[Data de consulta: Abril 2016]
- [7] Agencia de Informática y comunicaciones de la comunidad de Madrid; Métricas para Informes de Pruebas de Rendimiento.
http://www.madrid.org/arquitecturasw/images/documentacion/calidad/actual/generico/ucc_metricas_pruebas_rendimiento_v1.2.pdf
[Data de consulta: Maig 2016]

- [8] Amazon Web Service; NFS and CIFS Options for AWS:
<https://www.youtube.com/watch?v=xbuiIwEOCAs>
[Data de consulta:Abril 2016]

- [9] Amazon Web Service; Using Amazon Web Services and DFS
Replication for Disaster Recovery of File Servers.
<https://d0.awsstatic.com/whitepapers/implementing-windows-file-server-disaster-recovery.pdf>
[Data de consulta:Abril 2016]

- [10] Cloud Spectator, "Comparison among the 10 Top IaaS Providers", 2015.
[Data de consulta:Abril 2016]

APÈNDIX

A1. Topologia plantejada per a la nova infraestructura de l'empresa Sportife

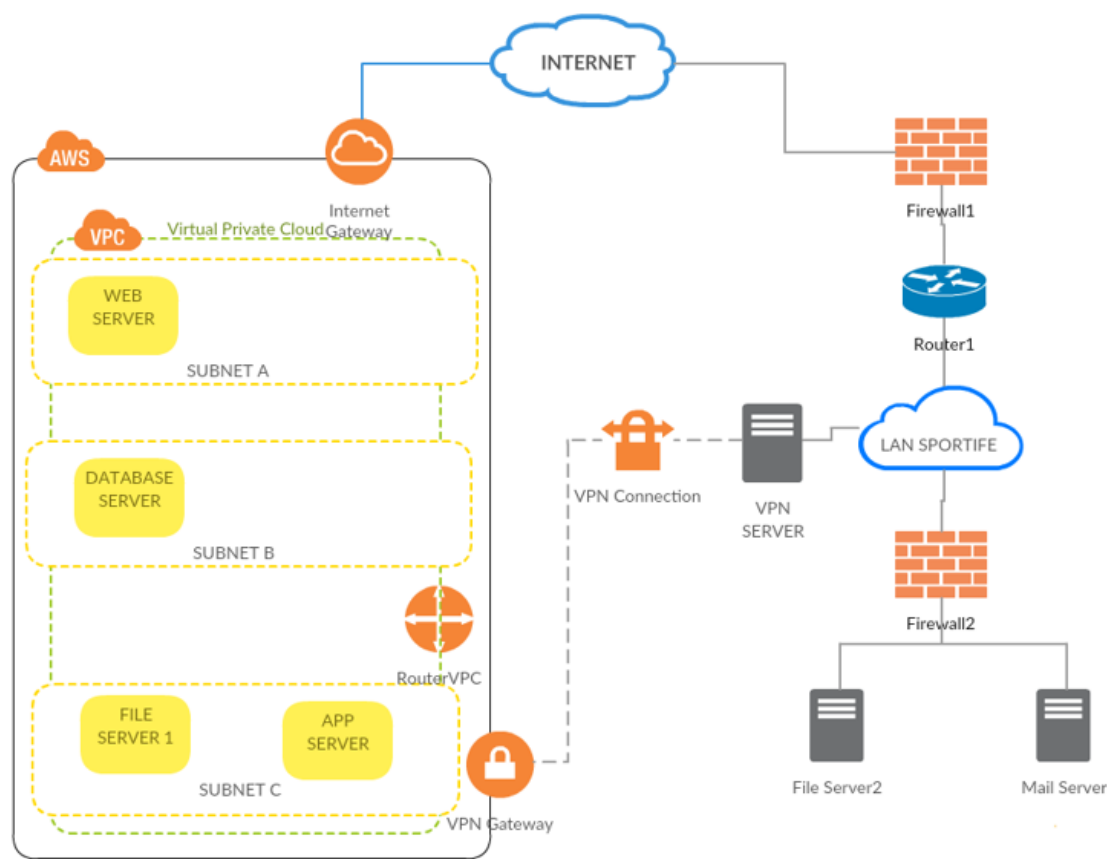


Fig12. Topologia final de l'empresa.

A2. Sortida del benchmark de la connexió TCP entre dues instàncies m3.large

```

ubuntu@ip-10-0-2-111:~/iperf$ sudo iperf3 -c 10.0.2.231 -i 10 -t 300 -V -p 80
iperf 3.1
Linux ip-10-0-2-111 3.13.0-74-generic #118-Ubuntu SMP Thu Dec 17 22:52:10 UTC 20
15 x86_64
Time: Sun, 26 Jun 2016 16:33:06 GMT
Connecting to host 10.0.2.231, port 80
Cookie: ip-10-0-2-111.1466958786.616830.5f40
TCP MSS: 8949 (default)
[ 4] local 10.0.2.111 port 50049 connected to 10.0.2.231 port 80
Starting Test: protocol: TCP, 1 streams, 131072 byte blocks, omitting 0 seconds,
300 second test
[ ID] Interval           Transfer     Bandwidth       Retr   Cwnd
[ 4]  0.00-10.00 sec    1.19 GBytes  1.03 Gbits/sec   15    821 KBytes
[ 4] 10.00-20.00 sec    887 MBytes  744 Mbits/sec   12    787 KBytes
[ 4] 20.00-30.00 sec    887 MBytes  744 Mbits/sec   11    752 KBytes
[ 4] 30.00-40.00 sec    887 MBytes  744 Mbits/sec   11    717 KBytes
[ 4] 40.00-50.00 sec    887 MBytes  744 Mbits/sec   11    673 KBytes
[ 4] 50.00-60.00 sec    887 MBytes  744 Mbits/sec   11    629 KBytes
[ 4] 60.00-70.00 sec    887 MBytes  744 Mbits/sec   11    594 KBytes
[ 4] 70.00-80.00 sec    887 MBytes  744 Mbits/sec   10    804 KBytes
[ 4] 80.00-90.00 sec    887 MBytes  744 Mbits/sec   11    778 KBytes
[ 4] 90.00-100.00 sec   887 MBytes  744 Mbits/sec   11    734 KBytes
[ 4] 100.00-110.00 sec   887 MBytes  744 Mbits/sec   11    699 KBytes
[ 4] 110.00-120.00 sec   887 MBytes  744 Mbits/sec   11    655 KBytes
[ 4] 120.00-130.00 sec   887 MBytes  744 Mbits/sec   11    612 KBytes
[ 4] 130.00-140.00 sec   887 MBytes  744 Mbits/sec   10    830 KBytes
[ 4] 140.00-150.00 sec   887 MBytes  744 Mbits/sec   12    795 KBytes
[ 4] 150.00-160.00 sec   887 MBytes  744 Mbits/sec   11    760 KBytes
[ 4] 160.00-170.00 sec   887 MBytes  744 Mbits/sec   11    717 KBytes
[ 4] 170.00-180.00 sec   887 MBytes  744 Mbits/sec   11    682 KBytes
[ 4] 180.00-190.00 sec   887 MBytes  744 Mbits/sec   11    638 KBytes
[ 4] 190.00-200.00 sec   887 MBytes  744 Mbits/sec   11    594 KBytes
[ 4] 200.00-210.00 sec   887 MBytes  744 Mbits/sec   10    804 KBytes
[ 4] 210.00-220.00 sec   887 MBytes  744 Mbits/sec   11    778 KBytes
[ 4] 220.00-230.00 sec   887 MBytes  744 Mbits/sec   11    743 KBytes
[ 4] 230.00-240.00 sec   887 MBytes  744 Mbits/sec   11    708 KBytes
[ 4] 240.00-250.00 sec   887 MBytes  744 Mbits/sec   11    664 KBytes
[ 4] 250.00-260.00 sec   887 MBytes  744 Mbits/sec   11    620 KBytes
[ 4] 260.00-270.00 sec   887 MBytes  744 Mbits/sec   11    594 KBytes
[ 4] 270.00-280.00 sec   887 MBytes  744 Mbits/sec   10    804 KBytes
[ 4] 280.00-290.00 sec   887 MBytes  744 Mbits/sec   11    760 KBytes
[ 4] 290.00-300.00 sec   887 MBytes  744 Mbits/sec   11    725 KBytes
-----
Test Complete. Summary Results:
[ ID] Interval           Transfer     Bandwidth       Retr
[ 4]  0.00-300.00 sec   26.3 GBytes  754 Mbits/sec   332
[ 4]  0.00-300.00 sec   26.3 GBytes  753 Mbits/sec
CPU Utilization: local/sender 1.1% (0.1%u/0.9%u), remote/receiver 5.1% (0.3%u/4.8%u)

```

Fig13. Sortida de la comanda iperf per a testear l'ample de banda d'una instància M3.large

A3. Fitxa tècnica de les instàncies EC2 contractades per a allotjar els serveis cloud.

Tipus d'instància	M4.xlarge
Hardware	CPU: Intel Xeon® E5-2676 v3 (Haswell) , 2,4 GHz Nº cpus: 4 RAM: 16 GB Emmagatzematge: 80 GB SSD
Hostname	DatabaseServer
IP	10.0.3.10
Descripció	Aquesta instància allotjarà la Base de dades de l'empresa.
Preu mensual	\$83.4 +\$8.8 EBS
Tipus d'instància	D2.xlarge
Hardware	CPU: Intel Xeon® E5-2676 v3 (Haswell) , 2,9 GHz Nº cpus: 8 RAM: 30 GB Emmagatzematge: 12 TB muntats en RAID 0 (SSD)(EBS)
Hostname	FileServer
IP	10.0.4.11
Descripció	En aquesta instància s'hi instal·larà el servidor de fitxers de l'empresa, Les instàncies de tipus D2 estan pensades per a oferir alt rendiment en l'emmagatzematge i per utilitzar-les en sistemes d'arxius distribuïts
Preu mensual	\$372.94
Tipus d'instància	M4.large
Hardware	CPU: Intel Xeon® E5-2676 v3 (Haswell) , 2,4 GHz Nº cpus: 2 RAM: 8 GB Emmagatzematge: 120 GB (SSD)(EBS)
Hostname	WebServer
IP	10.0.2.10
Descripció	Instància on s'allotjarà el servidor web, s'ha optat per una instància M4.large reduint l'espai d'emmagatzematge respecte al servidor web actual.
Preu mensual	\$29.49 + \$13,2 EBS
Tipus d'instància	M3.large
Hardware	CPU: Intel Xeon E5-2670 v2 (Ivy Bridge) , 2,4 GHz Nº cpus: 2 RAM: 7.5 GB Emmagatzematge: 32 GB SSD
Hostname	App_Server
IP	10.0.4.11
Descripció	En aquesta instància s'allotjaran la aplicació de inventari que utilitza la empresa.
Preu mensual	\$48.5

Fig14. Instàncies contractades a la VPC.